

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-312326

(43)Date of publication of application : 25.10.2002

(51)Int.Cl. G06F 15/00
 G06F 1/00
 G06F 12/14

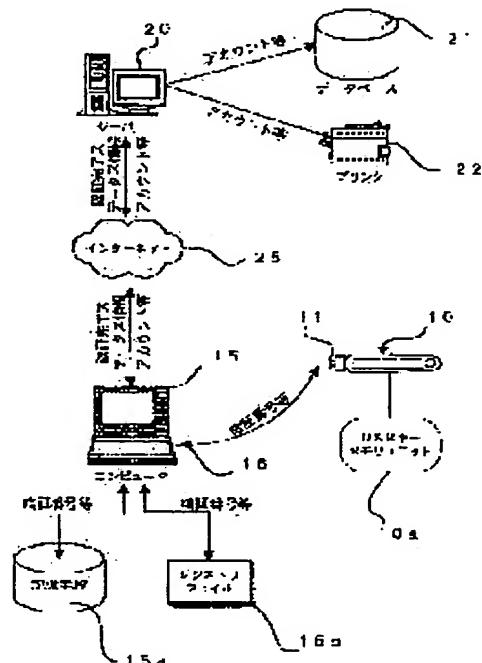
(21)Application number : 2001-118691 (71)Applicant : SMART CARD TECHNOLOGIES:KK
 (22)Date of filing : 17.04.2001 (72)Inventor : TAKEMURA KAZUO

(54) MULTIPLE AUTHENTICATION METHOD USING ELECTRONIC DEVICE WITH USB INTERFACE

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a multiple authentication method capable of easily controlling an account and a password, securing high security level, and being applied to various authentication subjects such as a server and a device.

SOLUTION: This multiple authentication method uses an electronic device with an USB interface composed of an account ID authenticating process for reading an account ID from a registry file 15b or a storage means 15a of a target computer 15 and checking the same by the electronic device 10, the computer authentication process, the completion of authentication status information indicating an event that the authentication is completed in both authentication processes, and an access and use rights authentication requiring process for transmitting the account and the password written in a memory unit 10a to the computer 15 as the target of the electronic device or the server 20 or the device 22 connected to the computer 15 by the electronic device 10.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's
decision of rejection]

[Date of extinction of right]

(51) Int.Cl. ⁷	類別記号	F I	テ-マ-ト ⁸ (参考)
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00	3 3 0 C 5 B 0 1 7
1/00	3 7 0	1/00	3 7 0 E 5 B 0 8 6
12/14	3 2 0	12/14	3 2 0 C

審査請求 未請求 請求項の数3 O.L (全8頁)

(21)出願番号 特願2001-118691(P2001-118691)

(22)出願日 平成13年4月17日 (2001. 4. 17)

(71)出願人 399001657

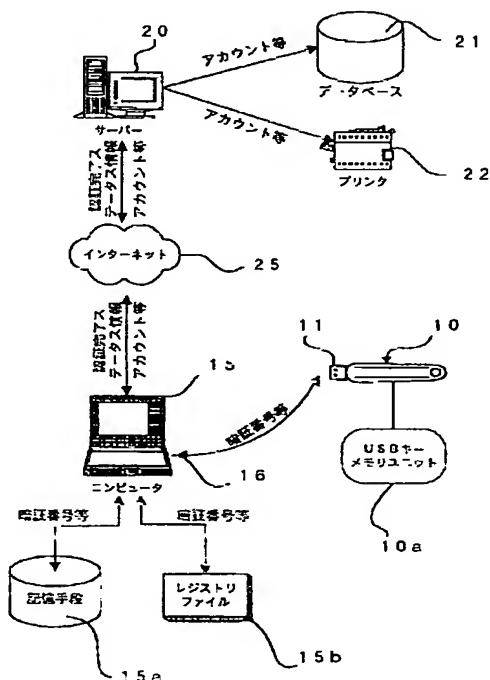
株式会社スマートカードテクノロジーズ
千葉県千葉市美浜区中瀬2-6(72)発明者 竹村 和夫
東京都中央区八丁堀2丁目11番7号 株式
会社スマートカードテクノロジーズ内(74)代理人 100071283
弁理士 一色 健輔 (外3名)
Fターム(参考) 5B017 AA03 BA05 BB09
5B085 AE01 AE11 AE23

(54)【発明の名称】 USBインターフェイスを備える電子デバイスを用いた複数認証方法

(57)【要約】 (修正有)

【課題】 アカウントやパスワードの管理が簡便であり、高いセキュリティレベルを確保し、サーバー、デバイスなどの多様な認証対象に適用可能な複数認証方法。

【解決手段】 電子デバイス10が挿入先コンピュータ15のレジストリファイル15bまたは記憶手段15aからアカウントIDを読み出して照合するアカウントID認証過程と、コンピュータ認証仮定と、両方の認証過程で認証が完了した事象を示す認証完了ステータス情報と、コンピュータ15に接続されるサーバー20やデバイス22などに、メモリユニット10aに書き込まれたアカウントおよびパスワードとを、電子デバイス10が当該電子デバイス挿入先のコンピュータ15しくはサーバー20やデバイス22に送信するアクセス・使用権認証要求過程とからなるUSBインターフェイスを備える電子デバイスを用いた複数認証方法。



【特許請求の範囲】

【請求項1】 コンピュータおよびこれに接続される各種サーバーやデバイス、並びに前記コンピュータまたは前記サーバーやデバイスにおいて起動されるアプリケーションプログラムの使用者について、前記コンピュータの備えるUSBポートに接続可能なUSB端子と、前記使用者を認証するに必要なアカウントやパスワード等の認証情報を記憶したメモリユニットと、前記USB端子を介した前記コンピュータとの前記認証情報の授受・照合処理をコントロールする制御チップセットとを備えたUSBインターフェイスを備える電子デバイスを用いて、その使用可否を判定する認証方法であって、前記電子デバイスのメモリユニットと、前記コンピュータの記憶手段およびレジストリファイルとに対して書き込み処理された、コンピュータ毎にその使用者と対応付けて設定された暗証番号から生成できるアカウントIDのうち、前記コンピュータの記憶手段またはレジストリファイルに書き込まれたアカウントIDについて前記電子デバイスが当該電子デバイス挿入先のコンピュータの記憶手段またはレジストリファイルから読み出して、読み出したアカウントIDと電子デバイス自身のメモリユニットに格納されている暗証番号から生成できるアカウントIDとを照合し、アカウントID自体の一致不一致を認証するアカウントID認証過程と、前記電子デバイスのメモリユニットと、前記コンピュータの記憶手段およびレジストリファイルとに対して書き込み処理された、コンピュータ毎にその使用者と対応付けて設定された暗証番号から生成できるアカウントIDのうち、前記記憶手段またはレジストリファイルに書き込まれたアカウントIDについて前記電子デバイスが当該電子デバイス挿入先のコンピュータの記憶手段から読み出して、読み出したアカウントIDと電子デバイス自身のメモリユニットに格納されている暗証番号から生成できるアカウントIDとを照合し、コンピュータと電子デバイスとの個別対応の正当性を認証するコンピュータ認証過程と、前記アカウントID認証過程およびコンピュータ認証過程における認証が完了した事象を示す認証完了ステータス情報と、前記コンピュータに接続される各種サーバーやデバイス、並びに前記コンピュータやサーバー等において起動されるアプリケーションプログラムの各々に設定され電子デバイスの前記メモリユニットに書き込まれたアカウントおよびパスワードとを、前記電子デバイスが当該電子デバイス挿入先のコンピュータもしくは前記サーバーやデバイスに送信し、これらサーバーやデバイスならびにアプリケーションプログラムに関するアクセス権および使用権について認証要求するアクセス・使用権認証要求過程とを有することを特徴とするUSBインターフェイスを備える電子デバイスを用いた複数認証方法。

【請求項2】 前記電子デバイスのメモリユニットに書き込まれている、当該電子デバイスに対応するコンピュータがサーバーへ最後に正当なアクセスをした最終接続情報を、前記アクセス・使用権認証要求過程において前記コンピュータもしくは前記サーバーやデバイスに送信することを特徴とする請求項1に記載のUSBインターフェイスを備える電子デバイスを用いた複数認証方法。

【請求項3】 前記暗証番号に加えて他の付帯番号を前記電子デバイスおよびコンピュータに格納し、この暗証番号および付帯番号からアカウントIDもしくはアカウントIDと付帯IDを生成して、前記アカウントID認証過程およびコンピュータ認証過程におけるアカウントIDの照合を行うことを特徴とする請求項1または2に記載のUSBインターフェイスを備える電子デバイスを用いた複数認証方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明はWEBサーバーやASPサーバーなどのサーバコンピュータ、プリンタなどの各種デバイス、およびそれらにおいて起動するアプリケーションプログラムにコンピュータを通じてアクセスする可否を認証する認証方法に関し、特にUSBキーなどのUSBインターフェイスを備える電子デバイスを用いた複数認証方法に関する。

【0002】

【従来の技術】堰を切ったようにあらゆる業種・業界においてEコマースサイトが立ち上がり、最近ではコンピュータとそれを結ぶネットワークが企業といわず個人といわず巷にあふれている印象が強い。このように、一般的な個人が容易にコンピュータに触れ、誰もが利用しやすいネットワーク環境が整いつつある現況において、ネットワークを含めたコンピュータシステムのセキュリティ管理が重要視されてきている。そこで、着目されるのがコンピュータやネットワークへの不正アクセスやそれにともなうデータの盗用・改変・破壊を防止する認証技術である。

【0003】従来の認証技術においては、マルチユーザーのコンピュータ・システムやネットワーク・システムを使用する際に正当な使用者たる本人であることを確認するためにユーザーIDとパスワードの組み合わせ入力によって認証が実行されていた。使用者がコンピュータ・システムやネットワークにログ・インする際に、ユーザーIDとパスワードのデータを入力すると、それがあらかじめアクセス権限リストに登録されたものかどうかの確認（認証）がなされ、認証された場合にのみシステムの使用が許可されることになる。このとき、アクセス権限リストに登録されたレベルのアクセス権限をユーザーに与える。

【0004】

【発明が解決しようとする課題】ところが、上記のよう

な従来手法による認証では新たに別の問題が浮かんできた。例えば、悪意の第三者によるパスワード等の盗用や解析を防ぎたいと考えるあまりにアカウントやパスワードを頻繁に変更したり大幅な桁数増加を図るすれば、その管理が使用者本人にも難しくなる問題がある。認証のたびにそれらの桁数の多いパスワード等を手動で入力するのは非常に面倒であるし、頻繁に変更するパスワード等を、多岐にわたる認証対象毎に確実に記憶しておくのは至難の業である。ましてやその認証ステップや桁数が多いとなれば使用者本人の記憶の中だけで管理するのにはます不可能であろう。

【0005】この場合、メモ帳などに認証対象の種類や変更のたびごとに暗証番号などを記入して当初はそれを逐次参照するしかないが、紙など視認性のある媒体に記録した瞬間に盗用のおそれが生じる。このためこのような手法が適用される状況としては、機密性のそれほど高くないデータしか取り扱わない企業向けや、一人暮らしの個人が密室において遊びでコンピュータを使用するといった、低度のセキュリティレベルしか要しない場面に限定されることになる。

【0006】また、コンピュータに付帯するキーボード等の入出力インターフェイスを用いて上記パスワードなどの入力作業を行うわけであるが、例えばそこでタイピングした文字・記号のキャラクターデータを経時記録しておき、第三者が後に当時のタイピング状況を再生可能とするプログラムや、目的のサーバーになりすまして偽のWeb画面データをターゲットのコンピュータに送信し、そこで入力されたアカウントやパスワードを抽出して盗用するといった手の込んだケースも存在する。

【0007】一方、使用者が自らのコンピュータにおいて一度入力したアカウントとパスワードはブラウザやOSなどのパスワード記憶機能などによってコンピュータ内に保存可能である。この機能が使用するレジストリファイルなどを第三者が発見するのは容易であるし、もしコンピュータごと盗難された場合にはパスワードなど一切知らずとも各種サーバーやアプリケーションプログラム等に対しアクセス・使用可能となってしまうおそれもある。いずれにせよ、アカウントやパスワードの手入力を省略してもしなくとも、セキュリティ面から言えば抜け穴は多く用意されていたのである。

【0008】本発明はこのような事情に鑑みてなされたものであって、アカウントやパスワードの管理が簡便でありながらも高いセキュリティレベルを確実に確保し、サーバー、デバイス、およびアプリケーションプログラムといった多様な認証対象に幅広く適用可能であるUSBキーを用いた複数認証方法を提供することを目的とする。

【0009】

【課題を解決するための手段】この発明は上記目的を達成するためになされたもので、第1の発明は、コンピュ

ータおよびこれに接続される各種サーバーやデバイス、並びに前記コンピュータまたは前記サーバーやデバイスにおいて起動されるアプリケーションプログラムの使用者について、前記コンピュータの備えるUSBポートに接続可能なUSB端子と、前記使用者を認証するに必要なアカウントやパスワード等の認証情報を記憶したメモリユニットと、前記USB端子を介した前記コンピュータとの前記認証情報の授受・照合処理をコントロールする制御チップセットとを備えたUSBインターフェイスを備える電子デバイスを用いて、その使用可否を判定する認証方法であって、前記電子デバイスのメモリユニットと、前記コンピュータの記憶手段およびレジストリファイルとに対して書き込み処理された、コンピュータ毎にその使用者と対応付けて設定された暗証番号から生成できるアカウントIDのうち、前記コンピュータの記憶手段またはレジストリファイルに書き込まれたアカウントIDについて前記電子デバイスが当該電子デバイス挿入先のコンピュータの記憶手段またはレジストリファイルから読み出して、読み出したアカウントIDと電子デバイス自身のメモリユニットに格納されている暗証番号から生成できるアカウントIDとを照合し、アカウントID自体の一一致不一致を認証するアカウントID認証過程と、前記電子デバイスのメモリユニットと、前記コンピュータの記憶手段およびレジストリファイルとに対して書き込み処理された、コンピュータ毎にその使用者と対応付けて設定された暗証番号から生成できるアカウントIDのうち、前記記憶手段またはレジストリファイルに書き込まれたアカウントIDについて前記電子デバイスが当該電子デバイス挿入先のコンピュータの記憶手段から読み出して、読み出したアカウントIDと電子デバイス自身のメモリユニットに格納されている暗証番号から生成できるアカウントIDとを照合し、コンピュータと電子デバイスとの個別対応の正当性を認証するコンピュータ認証過程と、前記アカウントID認証過程およびコンピュータ認証過程における認証が完了した事象を示す認証完了ステータス情報と、前記コンピュータに接続される各種サーバーやデバイス、並びに前記コンピュータやサーバー等において起動されるアプリケーションプログラムの各自に設定され電子デバイスの前記メモリユニットに書き込まれたアカウントおよびパスワードとを、前記電子デバイスが当該電子デバイス挿入先のコンピュータもしくは前記サーバーやデバイスに送信し、これらサーバーやデバイスならびにアプリケーションプログラムに関するアクセス権および使用権について認証要求するアクセス・使用権認証要求過程とを有することを特徴とするUSBインターフェイスを備える電子デバイスを用いた複数認証方法。

【0010】第2の発明は第1の発明において、前記電子デバイスのメモリユニットに書き込まれている、当該電子デバイスに対応するコンピュータがサーバーへ最後

に正当なアクセスをした最終接続情報を、前記アクセス・使用権認証要求過程において前記コンピュータもしくは前記サーバーやデバイスに送信することを特徴とするUSBインターフェイスを備える電子デバイスを用いた複数認証方法。

【0011】第3の発明は、第1または第2の発明において、前記暗証番号に加えて他の付帯番号を前記電子デバイスおよびコンピュータに格納し、この暗証番号および付帯番号からアカウントIDもしくはアカウントIDと付帯IDを生成して、前記アカウントID認証過程およびコンピュータ認証過程におけるアカウントIDの照合を行うことを特徴とするUSBインターフェイスを備える電子デバイスを用いた複数認証方法。

【0012】

【発明の実施の形態】==電子デバイスとしてのUSBキーの構造==

USB (Universal Serial Bus)は、パーソナルコンピュータ向けのシリアル・インターフェース規格であって、係る規格に準拠した機器(USB機器)とコンピュータとの接続をコンピュータ側が自動的に認識するプラグ・アンド・プレイ機能や、パーソナルコンピュータや機器の電源を入れたままUSBコネクタの抜き差しが可能となるホット・プラグ機能を可能にしている。また、ある程度までの電源の確保も接続先のコンピュータ等から行うことが出来るため機器自体の小型化を図ることができ、前述の接続処理のし易さとあいまって、扱いやすさの点で非常に優れている。本発明において使用される電子デバイスとしてのUSBキーは前述の機能を備えた上で、複数段階にわたる認証処理を実行可能なよう設計されている。

【0013】図1はUSBキー10の外形と使用形態の一例を示す説明図である。本発明の複数認証方法に用いられるUSBキー10は、外形的には図に示すようなパーソナルコンピュータなど各種コンピュータ15の備えるUSBポート16に接続可能なUSB端子11と、このUSB端子11の端部を固定するとともに人が把持しやすく携帯に便利な例えはスティック状などの種々の形状およびサイズで内部の電子ユニットを衝撃等から保護可能な強度を備えるケーシング12とからなっている。

【0014】一方そのケーシング12内部には、コンピュータ15の使用者を認証するに必要なアカウントやパスワード等の認証情報を記憶したメモリユニットと、USB端子11を介したコンピュータ15との前記認証情報の授受・照合処理をコントロールする制御チップセットとを備えている。両者を一体としたICチップセットなどを想定することもできる。また、前記ケーシング12とメモリユニットとを構造的に連結し、ケーシング12をこじ開けるとメモリユニット(もしくはメモリ内容)が破損されるようにすれば、セキュリティ性がより向上するであろう。当然、メモリユニット内に書き込ま

れている前記認証情報は暗号化されていることが好ましい。

【0015】==本発明を実現するシステム構成==

図2は本発明の複数認証方法を実現するシステム構成例を示す説明図である。以下、上記USBキー10を用いた複数認証方法を実際に運用するシステム構成について説明する。ここでは、予め契約した会員だけにアクセスを許すサーバー20が、インターネット25を介して前記会員のコンピュータ15へ各種のアプリケーションプログラムの提供を行うASP(Application Service Provider)として機能する状況を想定する。ASPとして前記サーバー20が役割を担う際には、当然のことながら会員認証を行って、アクセスする者の正当性を検証しなければならない。一方でその会員らは、サーバー20へのアクセスの度に要求される認証処理に逐次対応する必要がある。そこで本発明のUSBインターフェイスを備える電子デバイス(例:USBキー)を用いた複数認証方法をこの状況に適用し、前記サーバー20やそこで提供されるアプリケーションプログラムに設定されたアカウントやパスワードの管理を簡便化し、かつ高いセキュリティレベルを確保することとする。

【0016】サーバー20は、前述したようにインターネット25などの情報通信ネットワークに接続し、ASPサーバー、Webサーバーおよび電子メールサーバーとして機能する。また、当サーバー20の運営者側と契約を交わし会員となった者の個別データをカタログ化して管理する。この個別データには、各会員毎にアカウントが付されて管理され、このアカウントをベースにした、氏名(名称)、契約内容、取引履歴、パスワード等との関係表が作成されている。なおこの関係表における各種情報は前記USBキー10の適宜なメモリに格納される場合もある。

【0017】他に、会員に提供するアプリケーションプログラムが格納されたデータベース21を有し、その管理を行っている。ここに格納されるアプリケーションプログラムとしては、複雑なノウハウを凝した金融工学的計算や科学技術計算、企業における給与計算や税務処理などを実行するプログラムが考えられるが、ASPの業態等に応じて様々である。このようなアプリケーションプログラムは、会員のコンピュータ15からインターネット25を通じてサーバー20に送られてくるリクエストに応えて実行されるものであり、会員は実行に必要なデータのみをサーバー20に送信することで、例えばサーバー20が実行した複雑で膨大な計算によって得られた処理結果のみを受け取ることができる。勿論、アプリケーションプログラムを使用させるといったASPとしての機能だけでなく、プリンタ22やカメラなど各種デバイスを使用させる機能を設定してもよい。

【0018】上記サーバー20にインターネット25な

どを介してアクセスするのがコンピュータ15である。このコンピュータ15は使用者（会員）毎に暗証番号などを決めて使用権が設定されるため、コンピュータ起動時などにこの使用権の有無を確認する認証作業を行う必要がある。1台のコンピュータ15に1人のみ使用権を設定するか複数人の使用権を設定するかは、暗証番号などの認証情報をいくつ発行するかで容易にコントロールできる。また、ハードディスクドライブなどの適宜な記憶手段15aを備え、ここにOSやブラウザ、メールソフトなど各種アプリケーションをインストールしている。一般にこの記憶手段15a内に、各種の環境設定やドライバの指定、アプリケーションの関連づけなどの情報を保存するレジストリファイル15bが格納されている。本発明において、これら記憶手段15aとレジストリファイル15bとには使用者毎に設定された暗証番号が記録されている。

【0019】上記コンピュータ15のUSBポート16に接続されるのが前記USBキー10であり、USB端子11を介してメモリユニット10aに書き込まれている暗証番号から生成できるアカウントIDをコンピュータ15と授受し照合する。

【0020】なお、コンピュータ15は一般的なパソコン用コンピュータなどに限定されるものではなく、インターネット接続機能を備えた携帯電話機やTV受像器、ファックス機など様々なコンピュータ機器を、USB接続可能であることを条件に適用することが出来る。

【0021】==実施手順==

図3は本発明の複数認証方法の実際手順を示す流れ図である。上で述べたようにサーバー20がASPサーバーとして機能するものとして以下に本発明の複数認証方法の実施手順を説明する。まずサーバー20を運営するASP業者と契約し登録された各会員について認証情報を設定する必要がある（ステップs200）。必要な認証情報としては、アカウント、パスワード、および暗証番号である。アカウントとパスワードについては、サーバー20に会員のコンピュータ15がログインする際のサーバーログイン用のものと、このサーバー20を通じて使用するアプリケーションプログラムやそれを格納したデータベース21およびプリンタ22などのデバイス等の各使用権を確認する使用権確認用のものとがある。他方、暗証番号は前記会員毎に設定されるものであって、当該使用者が使用するコンピュータ15とUSBキー10との使用権についての対応確認に用いられる。

【0022】前記暗証番号は読みとられても容易に流用されないよう暗号化処理が施され、コンピュータ15の記憶手段15aおよびレジストリファイル15bに対して書き込み処理される（ステップs201）。次に、前記暗証番号と、ステップs200で設定されたサーバーログイン用および使用権確認用のアカウント・パスワードとを、USBキー10のメモリユニット10aに登録

する（ステップs202）。前記暗証番号から生成されるアカウントIDによりUSBキー10の所持者である会員と当該会員が使用するコンピュータ15との正当な使用関係が後に認証されることになる。

【0023】そして、USBキー10に対応するコンピュータ15がサーバー20へ一度でも正当なアクセスをしたことがあれば、その最終接続情報（例えば最終のクッキー情報）を、前記コンピュータ15の例えは記憶手段15a内から取得し、該当するUSBキー10のメモリユニット10aに書き込み処理をする（ステップs203）。サーバー20へのアクセス初回である場合には、USBキー10が予め備える固有情報でもってこの最終接続情報の書き込み処理は免除されるとすれば好適である。ここまででのステップにてアカウント、パスワード、暗証番号、クッキーといった認証に必要な情報の設定と、各機器への書き込みが完了する。

【0024】以後、コンピュータ15を起動した（ステップs204）前記会員がサーバー20にアクセスすることを試みる。この会員は、起動されたコンピュータ15のUSBポート16に、自ら所持するUSBキー10を挿入する（ステップs205）。コンピュータ15のOSはアラグ・アンド・プレイ機能によりUSBポート16に挿入されたUSBキー10の認識を始める。そしてコンピュータ15のシステムへの認識・組み込みが完了したUSBキー10は、コンピュータ15の記憶手段15aまたはレジストリファイル15bへアクセスする。そしてそこに記録されている前記暗証番号からアカウントIDを抽出し、自身のメモリユニット10aに格納されている暗証番号から生成できるアカウントIDと照合する（ステップs206：アカウントID認証過程）。

【0025】この暗証番号の照合により暗証番号から生成されたアカウントID自体の一一致不一致をみる。また、記憶手段10aからも暗証番号から生成できるアカウントIDを抽出・照合する（ステップs207：コンピュータ認証過程）。これらのステップs206、s207におけるアカウントIDの照合によりUSBキー10とコンピュータ15との対応関係の正当性とアカウントIDの正当性とを認証する。いずれかのステップにてアカウントIDの不一致をみた場合、USBキー10の制御チップセットは、コンピュータ15に対してそのOSに組み込まれた電源制御機能や各種入力機能の制限を命令し、正当とは認められない者のコンピュータ15の使用を差し止める。

【0026】アカウントID認証過程およびコンピュータ認証過程における認証が正常に完了した場合（ステップs208）、その完了事象を示す認証完了ステータス情報がUSBキー10またはコンピュータ15により発行される（ステップs209）。この認証完了ステータス情報は、例えはある会員に設定された暗証番号から生

成されるアカウントIDについて、対応するコンピュータのレジストリファイルおよび記憶手段において一致が認められた旨のテキストデータが圧縮・暗号化されているものである。この情報の発行は、USBキー10とコンピュータ15との関係が、使用者たる会員の正当性の面でも、暗証番号由来のアカウントIDの正当性の面でも認証されたことを意味する。つまり、権利的に何ら問題ない使用者が、予め定められたコンピュータ15を正当に使用している状況を指し示す。

【0027】認証完了ステータス情報を発行したUSBキー10は、この認証完了ステータス情報、自身のメモリユニット10aに書き込まれた前記アカウントおよびパスワード、および前記クッキー情報を、当該USBキー挿入先のコンピュータ15とインターネット25でつながったサーバー20やデバイスに送信する（ステップs210）。これによりこれらサーバーやデバイスは、送られてきたアカウント等の情報を受けて自身が保持しているアカウント等との照合作業を開始することになる。これをアクセス権および使用権についての認証要求とする（ステップs211：アクセス・使用権認証要求過程）。

【0028】サーバー20側では認証完了ステータス情報を読みとてどの会員がどのコンピュータから正当にアクセスを試みているのか認識する。と同時に、サーバーログイン用のアカウント・パスワード、ならびにクッキー情報の一致を認証すればアクセスを許可する。本実施例では、ASPサーバーとしてサーバー20が機能するから、サーバー20の記憶手段21に格納されている各種アプリケーションプログラムの使用権についてのアカウント・パスワード認証も実施する。サーバー20側での認証が全て正常に完了すればアクセス・使用権認証通知がコンピュータ15に送信される。コンピュータ15およびUSBキー10では前記のアクセス・使用権認証通知を受信し（ステップs212）、認証完了となる（ステップs213）。

【0029】なお、前記アカウントID認証過程およびコンピュータ認証過程において一致不一致の照合対象となつたアカウントIDは、両過程において全く同じものを用いても良いし、或いは各過程で由来が別のアカウントIDを用いるとしてもよい。

【0030】また、前記暗証番号に加えて他の付帯番号を前記電子デバイスおよびコンピュータに格納し、この暗証番号および付帯番号からアカウントIDもしくはアカウントIDと付帯IDを生成して、前記アカウントID認証過程およびコンピュータ認証過程におけるアカウントIDの照合を行うこととしても好適である。

【0031】====その他の実施例====

多様な認証手段を統合した複数認証としては、上記実施例のようなアカウントとパスワードおよび暗証番号から生成されるアカウントIDによるものに加え、ログイン

時に自動的にパスワードを生成するトークン、デジタル証明書、生体認証（指紋や虹彩走査）など多種多様な認証手段の組み合わせを適用することも考えられる。いずれにしてもこれらの認証情報をUSBキーのメモリユニットに格納しておけばよいのである。

【0032】

【発明の効果】以上に説明したように本発明のUSBインターフェイスを備える電子デバイスを用いた複数認証方法によれば、アカウントやパスワードを頻繁に変更したり、大きな桁数のそれらアカウントやパスワードを認証のたびごとに手入力することなく悪意の第三者によるパスワード等の盗用や解析を防ぐことが可能になる。しかも、たとえそれらアカウントやパスワードを頻繁に変更し、その上その桁数をどれだけ大きく複雑なものとしたとしても、アカウントやパスワード等は電子デバイスのメモリユニットに格納されるため、使用者本人はなんらその複雑さを意識することなく簡便に使用・管理することが出来るのである。

【0033】また、電子デバイスのメモリ内にパスワード等を記憶するために、メモ帳やノート、手帳といった視認性のある媒体に記録するのとは異なり、容易には盗み見られる状況は生じないし、かといってパソコン内のファイルにパスワード等を暗号化記録しておきながらパソコン起動前にそれを忘却すれば使用不可となるといった愚を犯すおそれもない。勿論、キーボード等の入出力インターフェイスにおけるタイミング情報を記録されてしまうおそれや、目的のサーバーになりすました偽サーバーがWeb画面で入力されたアカウントやパスワードを抽出盗用するといったおそれも全て解消される。

【0034】さらに上記の効果は、例えばコンピュータの起動から始まって当該コンピュータ内に格納されたアプリケーションプログラムやデータの使用、そして通信回線に接続してインターネットを介した所定サーバーへのアクセス、およびそこでのデータベースアクセスやアプリケーション使用に至るといった、多段階にわたる認証を通じて発揮されるものであり、その使用や管理の簡便性とセキュリティ性の高さは一貫している。

【0035】つまり、電子デバイスのメモリユニットにそれら各段階において必要となるアカウントやパスワードなどを格納しておけば、各認証段階を正常に完了してはじめて次の段階に進めるよう確実な複数認証が実行される一方、その実行は自動化され使用者に負担となる作業は一切要しないため極めて迅速に処理される。このため、本発明の複数認証方法は、各コンピュータやネットワークに必要とされるセキュリティ性の高低に関わらず様々な状況において適用することができ、その認証対象もコンピュータやサーバーおよびデバイスからアプリケーションプログラムまで実に幅広いものとなるのである。

【0036】しかして、アカウントやパスワードの管理

が簡便でありながらも高いセキュリティレベルを確実に確保し、サーバー、デバイス、およびアプリケーションプログラムといった多様な認証対象に幅広く適用可能であるUSBインターフェイスを備える電子デバイスを用いた複数認証方法を提供可能となる。

【図面の簡単な説明】

【図1】USBキーの外形と使用形態の一例を示す説明図である。

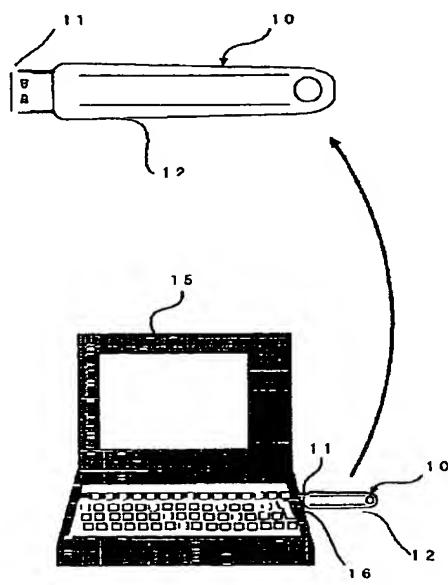
【図2】本発明の複数認証方法を実現するシステム構成例を示す説明図である。

【図3】本発明の複数認証方法の実際手順を示す流れ図である。

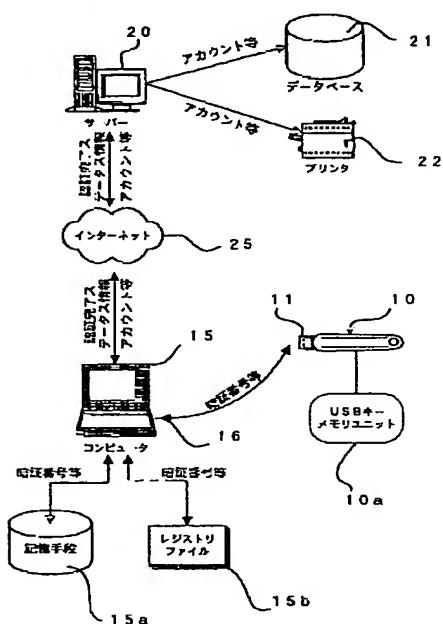
【符号の説明】

- 10 電子デバイス (USBキー)
- 10a メモリユニット
- 15 コンピュータ (挿入先コンピュータ)
- 15a 記憶手段
- 15b レジストリファイル
- 20 サーバー
- 22 デバイス (プリンタ)

【図1】



【図2】



【図3】

